Final Project Proposal

林峻賢 0711540

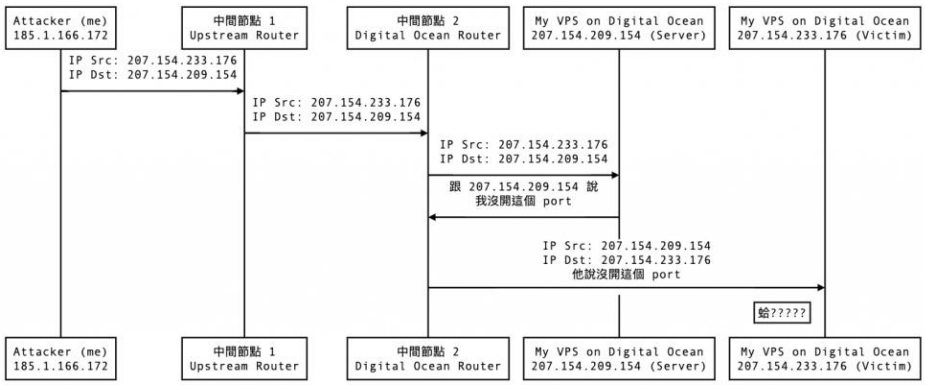
壹、 題目：IP Spoofing 模擬攻擊與防禦

貳、 動機

網路的誕生為了讓使用者可以更方便的與人交流資訊，因此設計之初的架構並未防範惡意攻擊，所以壞人可以透過這些漏洞進行惡意傳送封包，導致網路發生壅塞或癱瘓。在歷經數十年的攻擊與防禦後網路架構更加安全，而 IP spoofing 是時至今日仍然流行的攻擊手段之一，為了瞭解這個攻擊手段原理如何運作以及防範，我希望能藉由這個期末專題徹底理解，並實際應用課堂上學習的知識。

參、 實驗流程

建立三台 linux 虛擬機分別做為 attacker、server、victim client。Victim client 首次與 server 建立連線時，attacker 要設法去監聽到 client 的 source MAC address、source IP、destination IP 等等的相關資訊，attacker 知道以上這些資訊之後便可製作 spoofing packets，將這些 spoofing packets 送給 server，server 將會認為這些封包應屬於 victim client 發送的而將對其進行回應，而這樣便可以對 client 進行一輪的攻擊。



圖一

如圖一所示，attacker 以竊取得到的資訊製作出 spoofing packets 會送往 routers 進行 forwarding，spoofing packets 抵達 server 所處，server 便對其做出回應，但收到 response packets 是 victim client。

要對 IP spoofing 進行防禦可以使用 packet filtering，針對封包的

source IP 與實際 IP 不符時拒絕傳送。預計會使用 Python 實作，並且使用 scapy package 製作 spoofying packets。

肆、 參考資料

[1] Day 17 網路層攻擊實例 - IP Spoofing - iT 邦幫忙::一起幫忙解決難題，拯救 IT 人的一天 (ithome.com.tw)

[2] DDoS 防禦 - 海爾雲端 (highercloud.com.tw)